Cyber Security Landscape in Taiwan

Joy Chan
TW CERT/CC
26 November, 2018
A German Alexa owner returned home to find his Amazon device had started a 'party' at 2am, leading to police breaking down his door.
• An Amazon Echo in Hamburg started its own party on a recent Saturday morning, even though its owner was not home and hadn't activated Alexa.

• The loud music woke neighbors who called police. When the police arrived they had to break down the front door to turn off Alexa.

• The police changed the door lock, and the owner only found out when he arrived home and his key didn't work.
The impact is even bigger
- Boundary deconstruction, 3G/4G/5G
- Cloud Service, Smart IoT
- Cyber Physical Integration

**New ICT, New Challenges**

**Ubiquitous / IoT Security**

- M2M Security
- Cyber Physical Security
- Context Aware Threat Detection
- ICS Cybersecurity

**Cloud & Data Security**

- Cloud Security
- Data Security
- Security Governance
- Privacy Preserving
- Mobile Security

**Inter-networking Security**

- Anti-spam Mail
- VA, F/W, IDS, IPS
- PKI, VPN

**Web Service Security**

- Web App Firewall
- Web DB Security Monitor
- SIEM/Taint Analyzer
- DRM

**Critical infra Healthcare**

2004 2008 2012 2016 2018
Hacker’s attack & disaster expanded

showoff -> steal data -> damage -> economic crime -> political purpose

DarkSeoul cyber attack on South Korea

Electronic document system was intrusion, Taiwan

US Target was hacked by 18 m, 110 million confidential data was stolen, loss 420 million US dollars

Oil, power and water plants were attacked 257 times, USA

First Bank’s ATM was hacked, NT 83.3 million was picked up by theft without card

"Ransomware rages on Taiwan" the most appalling security attack of the year

2015 12/2

Taiwan 18 shopping site leak personal information, consumers are deceiving NT 90 million

2014 12/19

The German steer mill control system was compromised, leaving the furnace out of controlled and unrecoverable damage

Cool mobile phones, router & computers which made by China have been found the back door of a Trojan horse

2014 12/2 8

ec-council website was hacked, user sensitive be leaked

2014 12/15

Millions of IoT devices DoS attack Amazon, Twitter

2016 10/21

Far Eastern Bank SWIFT was hacked, stolen NT 1.8 billion

2016 10/3

"Ransomware rages on Taiwan" the most appalling security attack of the year

2016 2/24

First Bank’s ATM was hacked, NT 83.3 million was picked up by theft without card

2016 2/5

The German steer mill control system was compromised, leaving the furnace out of controlled and unrecoverable damage

Showoff & steal data & damage & economic crime & political purpose

Millions of IoT devices DoS attack Amazon, Twitter

Far Eastern Bank SWIFT was hacked, stolen NT 1.8 billion

2017 10/3

"Ransomware rages on Taiwan" the most appalling security attack of the year

First Bank’s ATM was hacked, NT 83.3 million was picked up by theft without card

"Ransomware rages on Taiwan" the most appalling security attack of the year
Security Solutions vs New Threats

Cyber Border Web App Security Mobile  Cloud & IoT Security

**Attack Vectors**
- **Virus** → **Worm** → **Botnet**
- **Mobile App Virus** + IoT Botnet
- **Phishing & Web Replace.** → **APT** → **Ransomware**

**Defense Solution**
- Anti-Virus + Firewall + IDS/IPS
- SOC + WAF + Email Protection → **Smart Defense**

**New ICT Application**
- Increasingly sophisticated attacking techniques
- Emerging ICT technologies change the vector of attacks
- Traditional defense efficiency is difficult to upgrade
- Lack effective defensive techniques to face emerging attacks

**1980~**
- PC popularity
- Internet rapid development

**2000~**
- Hacking attacks increase

**2010~**
- Smart IoT device Leap growth

Solutions are not ready
Challenges for New Digital Era

1. IoT applications inadequate security, affecting business, facilities and personal safety
   • Industry 3.0-> 4.0 · ICS Cyber Physical System (CPS) connection->Exposure of security vulnerabilities
   • Bank 2.0-> 3.0 · Diverse payment devices and transaction flow -> Counterfeit, identity theft risk of derivative transactions

2. Cloud services have privacy and security concerns
   • Enterprises rely on Google Drive, Dropbox and other services, more sensitive information leaks, malware quickly infected
   • Data open to the public, privacy leak doubts

3. Smart mobile and apps hidden security risks
   • Android OS, Apps and wireless comm. vulnerability causing confidential losses
   • Mobile devices may have malicious software or backdoor vulnerabilities
IoT devices are easily hack

- 7 x 24 hours continue operation
- Most without anti-virus mechanism
- Default or simple login password
- More internet services open
Hidden back door in Web camera

- Unsafe firmware or program

```bash
46 check_factory_mode()
47 {
48     factory_mode_file="/mnt/sd/jsw_factory_mode.txt"
49     
50     if [ -f $factory_mode_file ] && [ $CHECK_CID = "AHUA-000099-DGCEX" ]; then
51         echo "*************** JSW FACTORY MODE ***************"
52         factory_mode=1
54         if [ $fact_check ]; then
55             factory_static_eth0_ip=${factory_mode_ip}
56         fi
57         echo "factory_static_eth0_ip: ${factory_static_eth0_ip}";
58     else
59         echo "*************** NORMAL MODE ***************"
60         factory_mode=0
61     fi
62 }
```

hidden telnet back door (no password required)
Webcam was hacked...

Personal privacy exposure & factory production observed can be seen around the world

- Living room (Banqiao)
- Business Store (Dasi)
- Community Garage (Fengyuan)
- Factory Operation (Taipei)

https://www.insecam.org/en/bycountry/TW/
More IoT appliances exist vulnerability

**Smart TV / Media stream**
- Vizio Smart TVs (VF552XVT)
- Hisense Android TV (Google TV)
- ASUS Cube (Google TV)
- Amazon FireTV
- Smart media stream player: Vizio CoStar LT (ISV-B11)
- Sony BDP-S5100, Panasonic DMP-BDT230 (Blu-Ray Player)
- LG BP530 (Blu-Ray Player)
- Netgear Push2TV (PTV3000)

**Smart Energy:**
- Smart Plug: Belkin Wemo
- Greenwave Reality Smart Bulbs
- LG Smart Refrigerator (LFX31995ST)

**IoT Applications:**
- Wink Hub
- Motorola RAZR LTE Baseband
- Smart home "gateway"
- Home Automation Hub: Staples Connect
- Ooma Telo VOIP Router
- Samsung SmartCam
- Smart printer: Epson Artisan 700/800 printer
Hacking IoT devices rapid increase

Japan ICT-ISCA Analysis

150,000 attack source IPs

Include in 361 types of IoT
Beauty and Mourning brought by AI

• AlphaGo defeats Ke Jie, the most advanced player in the human
• Over the next decade, AI can surpass humanity in any task-oriented objective field (Li Kaifu, 李開復)
• Stephen Hawking - will AI kill or save humankind?
• Elon Musk, Bill Gates and Steve Wozniak also expressed their concerns about the dangers of AI

Source: BBC News

Source: Digital Times Magazine
AI Brings New Living and New Threat

1. Chatbot

- Chatbot may be taught bad
- Chatbot has risk of hacking and malicious use

2. Self-driving Car

- Sensor attack – Camera (LED spot)
- Remote Attack – Penetration into car control system

3. Drone

- UAV communication and positioning system may be hacked
Chatbot may be a Bad Girl?!

AI chat robot Tay, who was an innocent girl praising humankind, turned into a Anti Human position in less than 24 hours

- Tay is an experiment by Microsoft’s Technology and Research and Bing search engine teams to learn more about conversations. The bot was targeted at 18- to 24-year-olds in the U.S. and meant to entertain and engage people through casual and playful conversation, according to Microsoft’s website. Tay was built with public data and content from improvisational comedians.

- Tay, who had been online for less than a day, fell ill under the guidance of Twitter users, became a radical racial speaker, forcing Microsoft shut it off.


Risk of hacking, malicious use of Chatbot

Chatbot with AI becomes smarter and user friendly, accompanies with vulnerable to malicious phishing, whaling and clickjacking attacks

- **Technical attack**: Through the hacker tools (such as metasploit) to communicate with other chat robots to exchange information secret investigation, the goal is to master the chat robot related information, mining can be exploited security vulnerabilities.

- **Social engineering attack**: Collect data of targeted victims from big data in public sources (such as social media), Dark Web (purchased passwords or personal data), and write an "evil robot" program to interact with the victim.

Reference: Sage Group,
Self-Driving Automobile

Levels of Driving Automation

SAE J3016

Google Self-Driving Car (in experiment)

Advanced Driver Assistance System (ADAS)

Tesla

HUMAN DRIVER MONITORS DRIVING ENVIRONMENT

AUTOMATED DRIVING SYSTEM MONITORS DRIVING ENVIRONMENT

0 1 2 3 4 5

No Automation Driver Assistance Partial Automation Conditional Automation High Automation Full Automation

Src: Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)
Sensing Devices

Self-driving Automobile making decisions based on artificial intelligence to control driving, highly relying on various Sensor information and communications

Source: Blackhat
Self-Driving Attack

- **Contactless Attacks (Sensors)**
  - Blinding Camera
  - Attacking Sensor
  - Attacking Radar
  - Attacking Lidar

- **Cyber Remote Attack**
  
  (hijack car control)
  - Hacking On-board Unit
  - Hacking Wireless Communication

*Source: Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)*
Sensor Attack – Camera (LED spot)

➢ Blinding Cameras – Results with LED spot

Attacking Cameras – Setup

- Attack: Blinding
- Interferers:
  - LED spot ($10)
  - Laser pointer ($9)
  - Infrared LED spot ($11)
- Cameras:
  - Mobileye, PointGrey

- Partial blinding
- Total blinding
  - LED toward the board
  - LED toward camera
  - Tonal Distribution

➢ Blinding Cameras – Results with Laser beam

- Total blinding

- Fixed laser beam
- Wobbling laser beam
- Damaged
- Permanently damaged

Src: Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)
Remote Attack - Penetration into car control system

Attack Paradigm:

1. Remote compromise
2. Gathering Vehicle Information
3. CAN Message analysis (in advance)
4. CAN message injection
   • Reprogram firmware
   • Functionality

Source: Blackhat
Amazon petitions the FAA to approve drone delivery tests
Attack UAV Communication & GPS

- Remote Control Drone Disruption
  - Invasion Wi-Fi communication, remote control
  - Can take off, spin clockwise, and land commands
- GPS Disruption
  (Transmit fake GPS signals)
  - GPS Spoofing
  - GPS Jammers
Evolution of Industrial Manufacture

**Industry 1.0**
Mechanical Production. Equipment powered by steam and water

**Industry 2.0**
Mass production assembly lines
Electrical, combustion engine, new material

**Industry 3.0**
Automated production using electronics & IT
Electronic, digital control, information system

**Industry 4.0**
Intelligent production incorporated with IoT, cloud, technology, & big data
Cyber Physical System

Source: MIC Research Report, III
Enterprise Security Solution Segments

Cyber defense matrix: Asset Classes (Vertical) & Operational Functions (Horizontal)

Ref: Sounil Yu (sounil@gmail.com) @ RSA Conference, III summary
Current research and development focus

Objectives:
Leverage AI to develop the application security integration Introduce to Digital Economy (smart city, smart manufacturing)
Conclusion?!........

- ICT Trends: IoT, Mobile, Cloud, and Big-Data Analysis
- Attacks are increasingly complex and emerging technologies change the face of attacks
- Insufficient design of safety and security, weak device protection, and concern for privacy, personal and national security, affecting the development of IoT
- Increased number of smart networking devices, failure of boundary detection and defense, the hidden weaknesses, data leakage and privacy disclosure concern
- Security challenges: Security defenses must be quick, comprehensive, and early detection (AI). Emerging technologies must integrate security services
President of R.O.C (Taiwan) Ing-Wen, Tsai

~The importance of Cybersecurity issues just as importance of national security issues~

-Source: HITCON Pacific, 2016

- Cybersecurity is one of the significant elements for digital economic
- Invest NT250 millions for Enhancing CIIP
- Cultivate cybersecurity talents
- Facilitate start-ups

Premier Lai in the concluded meeting
Gov. Initiatives with Industry & Academia

National Security Council

Executive Yuan

Industry Promotion

Talents Cultivation

Ministry of National Defense

Demands

Ministry of Economic Affairs

Subsidize

Startup

Field Trial

Field trial

Provide solution

Ministry of Education

Subsidize

Spin off

Research Center

Student

Ministry of Science & Technology

Innovative R&D Program

Ministry of Economic Affairs

Employed
What government project has been initiated?

The introduction of

「Taiwan Cyber Security Industry Flagship Project」
Cybersecurity Flagship Project Goals

Promoting information security industry with domestic R&D entrepreneur capability by means of national security demands and build up the whole Cyber Security industry chain.

**Talent Cultivation**

Cybersecurity talent cultivation for government, national defense, business, and CIIP.

**Advanced Technology**

Develop advanced cybersecurity technologies based on AI technology.

**Field Trial**

Build cybersecurity test bed for products verification.

**Environment Construction**

Build up domestic cybersecurity industry chain.
Out Reach Strategies

International Technology Cooperation

International Business Matching

Build up Domestic Cybersecurity Industry Eco-System
Lead Transformation and Innovation

Cybersecurity Talent Cultivation

Research and Development for Cybersecurity Solution and appliances

Field Trial Multiple Test Bed

Cybersecurity Market Needs Drive Supplies

Government Demand

Business Market

CIIP Market
Cybersecurity Test Bed

Taiwan Power Company
Power Plant

CPC Corporation, Taiwan
Oil Refinery

Taiwan Water Corporation
Water Purification Plant
Critical Infrastructure Platform

Energy

Water

Traffic

Telecom

Finance

Healthcare

Emergency

Gov.
Cyber Security Center-Taipei

- Taipei city will be surrounded by cybersecurity industry
- Taipei will be a smart city living lab, it will be a platform to demonstrate cybersecurity solution for startups.
- Taipei City will be a center of ISAC, which will cooperate with other 5 cities in Taiwan.

Industry Clustering  Strong Ecosystem  Living Lab
Cyber Security Solutions

Connecting academic research and developing core technologies

Forensics
Build probabilistic patterns by summarizing user’s sequential behaviors. Malware analysis (static/dynamic)

UEBA
Malicious activities detection based on monitoring the variance of different grouping condition

AI Intelligence Analysis

Ai Security

Threat Awareness
Detect the emerging cyber threats and vulnerabilities exploited worldwide

Analytics
Anomaly detection Threat profiling Malware detection

Cloud
Protect cloud service and detect insider and anomalous behavior

Probe
Explore vulnerabilities in IoT device and web portal
Thank you!